

Family list

2 family member for:

JP11219340

Derived from 1 application.

1 DEVICE AND SYSTEM FOR AUTHENTICATION MANAGEMENT

Publication info: **JP3587045B2 B2** - 2004-11-10

JP11219340 A - 1999-08-10

Data supplied from the **esp@cenet** database - Worldwide

THIS PAGE BLANK (USPTO)

DEVICE AND SYSTEM FOR AUTHENTICATION MANAGEMENT

Patent number: JP11219340
Publication date: 1999-08-10
Inventor: FUJII TERUKO; NAKAMURA HIROSHI; SADAKANE TETSUO; BABA YOSHIMASA
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
 - international: G06F15/00
 - european:
Application number: JP19980023042 19980204
Priority number(s): JP19980023042 19980204

Report a data error here

Abstract of JP11219340

PROBLEM TO BE SOLVED: To enable an administrator to freely set and consistently manage a security policy extending over plural authenticating means by providing a terminal information data base wherein information corresponding to authentication conditions that the plural authenticating means are optionally combined, is registered. **SOLUTION:** A terminal ID as an identifier indicating a terminal unequivocally is registered in a column R41 of the data structure of authentication conditions, that authenticating means of a terminal information data base are optionally combined and general authentication expressions showing the authentication conditions used for normal authentication for every terminals are registered in a column R42. Further, specific authentication expressions showing authentication conditions exclusive to a specific service and application are registered in columns R43 to R44. Thus, the authentication conditions used for the normal authentication and the authentication conditions used for the specific service and application are registered terminal by terminal distinctively in the terminal information data base and managed by an authentication management device.

	R41	R42	R43	R44	
	端末ID	一般認証式	特定 認証式1	特定 認証式2	...
G41	出退勤 管理装置	{ユーザID*指紋}+ ICカード	NULL		
G42	ドア制御 装置1	指紋	NULL		
G43	ドア制御 装置2	{指紋*ICカード}+ {声紋*ICカード}	NULL		
G44	パソコン1	ユーザID+	秘密管理=	NULL	
G45		パスワード	ユーザID+		
	パソコン2	ICカード+	秘密管理=	NULL	
		パスワード	NULL		
	...				

Data supplied from the esp@cenet database - Worldwide

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-219340

(43) 公開日 平成11年(1999) 8月10日

(51) Int.Cl.⁸

G 0 6 F 15/00

識別記号

3 3 0

F I

C 0 6 F 15/00

3 3 0 A

審査請求 未請求 請求項の数 8 O L (全 16 頁)

(21) 出願番号 特願平10-23042

(22) 出願日 平成10年(1998) 2月4日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 藤井 照子

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 中村 浩

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 貞包 哲男

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 弁理士 宮田 金雄 (外2名)

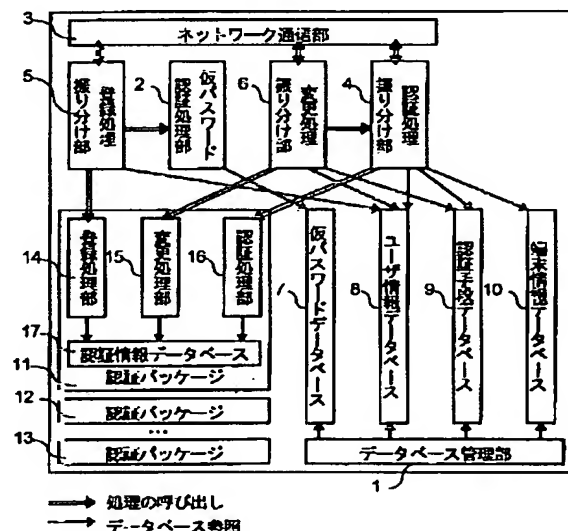
最終頁に続く

(54) 【発明の名称】 認証管理装置及び認証管理システム

(57) 【要約】

【課題】 管理者が複数の認証手段に跨るセキュリティ・ポリシーを自由に設定し、一貫して管理することができると共に、不正な認証情報の登録を回避して高度なセキュリティを必要とする場合にも適用でき、通常の認証と認証情報変更時の認証とを区別できる認証管理装置及び認証管理システムを得る。

【解決手段】 1又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、複数の端末の認証を管理するものであって、認証管理装置は、少なくとも、複数の端末に入力される認証情報に応じて認証処理を行う1又は複数の認証手段と、ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、認証手段に対応する情報が登録される認証手段データベースと、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備える。



【特許請求の範囲】

【請求項1】 1又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、上記複数の端末の認証を管理する認証管理装置において、少なくとも、上記複数の端末に入力される認証情報に応じて認証処理を行う1又は複数の認証手段と、上記ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、上記認証手段に対応する情報が登録される認証手段データベースと、上記認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えることを特徴とする認証管理装置。

【請求項2】 ユーザの上記認証情報を登録する際に参照される仮パスワードと当該仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、上記有効期限に応じて又は上記認証情報の登録に応じて上記仮パスワードデータベースから上記仮パスワードを削除することを特徴とする請求項1に記載の認証管理装置。

【請求項3】 上記認証手段データベースには、通常の認証で用いる一般認証時のしきい値と上記認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、上記認証手段は通常の認証には上記一般認証時のしきい値を用い、上記認証情報を変更する際には上記認証情報変更時のしきい値を用いて認証処理することを特徴とする請求項1又は請求項2に記載の認証管理装置。

【請求項4】 上記1又は複数の認証情報の少なくとも一つはバイオメトリクス認証情報であることを特徴とする請求項1、請求項2又は請求項3に記載の認証管理装置。

【請求項5】 1又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、上記複数の端末の認証を管理する認証管理装置を有する認証管理システムにおいて、上記認証管理装置は、少なくとも、上記複数の端末に入力される認証情報に応じて認証処理を行う1又は複数の認証手段と、上記ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、上記認証手段に対応する情報が登録される認証手段データベースと、上記認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えることを特徴とする認証管理システム。

【請求項6】 ユーザの上記認証情報を登録する際に参照される仮パスワードと当該仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、上記有効期限に応じて又は上記認証情報の登録に応じて上記仮パスワードデータベースから上記仮パスワードを削除することを特徴とする請求項5に記載の認証管理システム。

【請求項7】 上記認証手段データベースには、通常の認証で用いる一般認証時のしきい値と上記認証情報を変

更する際に用いる認証情報変更時のしきい値とを区別して登録でき、上記認証手段は通常の認証には上記一般認証時のしきい値を用い、上記認証情報を変更する際には上記認証情報変更時のしきい値を用いて認証処理することを特徴とする請求項5又は請求項6に記載の認証管理システム。

【請求項8】 上記1又は複数の認証情報の少なくとも一つはバイオメトリクスの認証情報であることを特徴とする請求項5、請求項6又は請求項7に記載の認証管理システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】この発明は、複数のシステムや端末の認証を管理する認証管理装置及びその認証管理装置を有する認証管理システムに関するものであり、例えば、ネットワークに展開される複数のシステムや端末のバイオメトリクス情報、パスワード等による個人認証を管理する認証管理装置及びその認証管理装置を有する認証管理システムに関するものである。

【0002】

【従来の技術】情報化社会の発達は、これまで利便性の追求の方向に進んできたが、インターネットの急速な普及は、セキュリティの向上を必要としている。コンピュータ社会におけるセキュリティの構成要素の1つが個人認証である。すなわち、情報やサービスを適切なユーザに対して与えるためには、そのユーザが誰であるかを確認することが必須であり、これを行うのが個人認証である。

【0003】従来からコンピュータシステムによる認証は、様々な場面で行われている。例えば、出退勤管理にはパンチカードに代わってICカードが用いられているし、また、セキュリティの高い部屋のドアの開閉にもICカードや磁気カードが用いられている。また、コンピュータ端末による各種サービスへのアクセスにはパスワードが多用されている。

【0004】しかし、パスワードは比較的第三者に漏洩しやすく、高度なセキュリティを必要とする場合での適用に問題があった。これに対して近年では、各種技術の進歩に伴い、指紋や声紋等のバイオメトリクス情報を用いた照合やワンタイムパスワード等、様々な認証手段が提案され、実用化されている。

【0005】例えば、従来のバイオメトリクス情報を用いた認証方法として、特開平8-16788号公報に開示された個人固有の複数の身体的特徴を用いる個人認証方法がある。この方法は、音声、指紋、筆跡等の個人固有の複数の特徴を読み取り、読み取った特徴パラメータをそれぞれ個人の特徴を反映する複数のカテゴリに分割し、分割した各カテゴリをその個人の特徴の現れ易さにより、重み付けを施して統合する。そして、統合により得られた各特徴パラメータをその個人の特徴の現れ易さ

により、重み付けを施して統合し、統合結果をしきい値と比較して本人確認を行う。

【0006】また、図14は、従来のバイOMETRICS情報を用いた認証機能を持つ一般的なサービス・サーバの構成を示すブロック図である。図中、サービス処理部31は、システムの主体となるサービスの処理を行う。例えば、出退勤管理システムでは出退勤管理の処理を行う。認証処理部32は、バイOMETRICS情報を用いた認証を行う。認証情報データベース33は、認証に用いられるバイOMETRICS情報を登録する。登録サービス処理部34は、バイOMETRICS情報を登録するための処理を行う。

【0007】次に動作について説明する。サービス・サーバに接続された端末からサービスの要求がある場合は、端末からバイOMETRICS情報と共にサービス要求信号が送信される。例えば、指紋情報と共に出退勤管理の要求信号が送信される。これらの情報を受け取ると、サービス処理部31は認証処理部32に認証処理を依頼する。認証処理部32は、端末から送信されたバイOMETRICS情報と認証情報データベース33に登録されているバイOMETRICS情報とを照合して認証OKか認証NGかを判定し、判定結果をサービス処理部31に通知する。サービス処理部31は通知された判定結果に従って、認証OKならサービスを実施し、認証NGならエラーを端末に通知してサービス要求に対する処理を終了する。

【0008】また、サービス・サーバに接続された端末からバイOMETRICS情報の登録要求がある場合は、端末からパスワードと共に登録要求信号が送信される。この情報を受け取ると登録サービス処理部34は、まず、パスワードのチェックを行う。その結果がOKなら、端末に対してバイOMETRICS情報の送信を要求する。その後、端末からバイOMETRICS情報が送信されると、登録サービス処理部34は、送信されたバイOMETRICS情報を認証情報データベース33に登録して登録要求に対する処理を終了する。

【0009】

【発明が解決しようとする課題】しかしながら従来の認証管理は、様々な条件の下で行われる様々な認証手段の認証を個々に管理するものであるため、管理者が複数の認証手段に跨るセキュリティ・ポリシーを自由に設定し、一貫して管理することができないという問題があった。セキュリティ・ポリシーとは、すなわち、使い勝手やシチュエーションに応じたセキュリティの強度に対する管理者の設計思想や運営についての考え方である。

【0010】また、例えばバイOMETRICS等の認証情報を登録する際には、パスワードを使用していたが、このパスワードは恒常的に有効であるため、このパスワードが漏洩した場合にはいつでも不正な認証情報を登録される可能性があり、高度なセキュリティを必要とする場

合での適用に問題があった。

【0011】また、登録されている認証情報を変更する際には、先に述べたパスワードを使用したり、その時点で登録されている認証情報を使用していたが、パスワードを使用する場合には、認証情報の登録の際と同様の問題があった。

【0012】さらに、登録されている認証情報を変更する際にその時点で登録されている認証情報を使用する場合には、通常の認証と認証情報を変更するための認証との区別がないため、より厳しいセキュリティが必要となる後者のセキュリティを特別に高くすることができないという問題があった。

【0013】この発明は上記のような問題点を解決するためになされたもので、管理者が複数の認証手段に跨るセキュリティ・ポリシーを自由に設定し、一貫して管理することができると共に、不正な認証情報の登録を回避して高度なセキュリティを必要とする場合にも適用でき、さらに、通常の認証と認証情報変更時の認証とを区別できる認証管理装置及び認証管理システムを得ることを目的とする。

【0014】

【課題を解決するための手段】この発明に係る認証管理装置は、1又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、複数の端末の認証を管理するものであって、少なくとも、複数の端末に入力される認証情報に応じて認証処理を行う1又は複数の認証手段と、ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、認証手段に対応する情報が登録される認証手段データベースと、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えるものである。

【0015】また、次の発明に係る認証管理装置は、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデータベースから仮パスワードを削除するものである。

【0016】また、次の発明に係る認証管理装置は、認証手段データベースに通常の認証で用いる一般認証時のしきい値と認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、認証手段は通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理するものである。

【0017】また、次の発明に係る認証管理装置は、1又は複数の認証情報の少なくとも一つはバイOMETRICSの認証情報であるものである。

【0018】さらにまた、この発明に係る認証管理システムは、1又は複数の認証情報を入力する複数の端末とネットワークを介して接続され、複数の端末の認証を管

理する認証管理装置を有するものであって、認証管理装置は、少なくとも、複数の端末に入力される認証情報に応じて認証処理を行う1又は複数の認証手段と、ユーザの認証情報に対応する情報が登録されるユーザ情報データベースと、認証手段に対応する情報が登録される認証手段データベースと、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースとを備えるものである。

【0019】また、次の発明に係る認証管理システムは、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデータベースから仮パスワードを削除するものである。

【0020】また、次の発明に係る認証管理システムは、認証手段データベースに通常の認証で用いる一般認証時のしきい値と認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録でき、認証手段は通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理するものである。

【0021】また、次の発明に係る認証管理システムは、1又は複数の認証情報の少なくとも一つはバイオメトリクスの認証情報であるものである。

【0022】

【発明の実施の形態】実施の形態1. 以下、本発明の認証管理システム及び認証管理装置に係る実施の形態1を説明する。図2に、本発明に係る認証管理システムの構成を示す。図中、認証管理装置21は、本発明の認証管理装置に相当し、複数の端末の認証を管理する認証管理装置である。端末22～24は、認証管理装置21からの認証管理に応じて各々のサービスをユーザに提供すると共に認証情報を入力する端末である。インタフェース装置25～27は、ユーザの認証情報を採取するマン・マシン・インタフェース装置である。ネットワーク28は、認証管理装置21と端末22～24間の通信を可能とするための通信ネットワークである。

【0023】また、図3に、この認証管理システムの一具体例を示す。図中、認証管理装置A1は、図2における認証管理装置21に相当する。出退勤管理装置C1、ドア制御装置C2～C3、勤怠管理装置C4、メールサーバC5は、それぞれ図2における端末22～24に相当する。テンキーパッドI1、指紋取得装置I2～I6、ICカードリーダI7～I9、声紋取得装置I10、パソコンI11～I15は、それぞれ図2におけるインタフェース装置25～27に相当する。

【0024】出退勤管理装置C1は出退勤を管理すると共にテンキー、指紋及びIC信号の認証情報を入力する装置であり、テンキーパッドI1、指紋取得装置I2、ICカードリーダI7が接続される。ドア制御装置C2

は比較的セキュリティの低い部屋へのドアを制御すると共に指紋の認証情報を入力する装置であり、指紋取得装置I3が接続される。ドア制御装置C3はセキュリティの高い部屋へのドアを制御すると共に指紋、声紋及びIC信号の認証情報を入力する装置であり、指紋取得装置I4、声紋取得装置I10、ICカードリーダI8が接続される。

【0025】勤怠管理サーバC4は勤務状況を管理するサーバであり、指紋取得装置I5～I6が接続され、指紋の認証情報を入力するパソコンI11～I12が接続される。メールサーバC5はメールの送受信を管理するサーバであり、IC信号の認証情報を入力するものを含むパソコンI11～I15が接続される。

【0026】テンキーパッドI1は、ユーザが0から9の10種類の数字を入力できるマン・マシン・インタフェース装置である。指紋取得装置I2～I6は、ユーザの指紋を読み取り、デジタルデータに加工するマン・マシン・インタフェース装置である。ICカードリーダI7～I9は、ICカード内の認証情報を読み出すマン・マシン・インタフェース装置である。声紋取得装置I10は、ユーザの声紋を取得し、デジタルデータに加工するマン・マシン・インタフェース装置である。パソコンI11～I12は、指紋取得装置I5～I6が接続されたパソコンである。パソコンI13～I14は、通常のパソコンである。パソコンI15は、ICカードリーダI9が接続されたパソコンである。

【0027】図3において、例えば、ユーザが出退勤管理装置C1のサービスを利用する場合、ユーザはテンキーパッドI1、指紋取得装置I2などを用いて認証用の認証情報を出退勤管理装置C1に入力しする。これに応じて、出退勤管理装置C1は入力された認証情報と共に認証コマンドをネットワークを介して認証管理装置A1に送信する。その後、認証管理装置A1は受信した情報に基づいて認証を行い、認証結果をネットワークを介して出退勤管理装置C1に送信する。そして、出退勤管理装置C1は認証結果に基づいて、認証OKの場合に、出退勤のデータを更新するなど、ユーザに対して独自のサービスを提供する。

【0028】また、図1に、図2における認証管理装置21の内部構成を示す。図中、データベース管理部1は、認証管理装置又は認証管理システムの管理者の指示にしたがって仮パスワードデータベース7、ユーザ情報データベース8、認証手段データベース9、端末情報データベース10の内容の管理を行う。

【0029】仮パスワードデータベース7は、ユーザの認証情報を登録する時の認証に用いる仮パスワードに対応する情報が登録されるデータベースである。ユーザ情報データベース8は、ユーザ個人の認証情報に対応する情報が登録されるデータベースである。認証手段データベース9は、端末に入力される認証情報に応じて認証処

理を行う認証手段である認証管理装置21内の認証パッケージに対応する情報が登録されるデータベースである。端末情報データベース10は、認証手段を任意に組み合わせた認証条件に対応する情報が登録されるデータベースである。

【0030】仮パスワード認証処理部2は、仮パスワードデータベース7を参照して仮パスワードによる認証を行う。ネットワーク通信部3は、ネットワーク28を介して端末22～24との通信を行うと共に、端末22～24から受信したコマンドの種類を判別する。

【0031】認証処理振り分け部4は、端末22～24から受信したコマンドが認証コマンドである場合、又は変更コマンドである場合に動作し、ユーザ情報データベース8でユーザの登録状況を確認し、認証手段データベース9で使用する認証パッケージを決定し、さらに端末情報データベース10で認証条件を決定して、所定の認証パッケージに認証処理を振り分けると共に、各々の認証パッケージの認証結果に基づいて認証を行う。

【0032】登録処理振り分け部5は、端末22～24から受信したコマンドが登録コマンドである場合に動作し、ユーザ情報データベース8でユーザの登録状況を確認し、仮パスワード認証処理部2にユーザの認証を依頼し、認証結果が真となった場合にユーザ情報データベース8に記載された認証パッケージにユーザの認証情報の登録を振り分ける。

【0033】変更処理振り分け部6は、端末22～24から受信したコマンドが変更コマンドである場合に動作する。ユーザ情報データベース8でユーザの登録状況を確認し、認証手段データベース9で認証パッケージの情報を確認し、認証処理振り分け部4にユーザの認証を依頼する。認証結果が真となった場合に該当する認証パッケージにユーザの認証情報の変更を振り分ける。

【0034】認証パッケージ11～13は、指紋照合、声紋照合、パスワード等、それぞれ異なる種類の認証を行うものであり、それぞれ、独自の登録処理部14、変更処理部15、認証処理部16、認証情報データベース17を持つ。登録処理部14は、インタフェース装置25～27で採取されたユーザ個人の認証情報を独自の認証情報データベース17に登録する。変更処理部15は、独自の認証情報データベース17に既に登録されている認証情報をインタフェース装置25～27で採取されたユーザの個人認証情報に変更する。認証処理部16は、インタフェース装置25～27で採取されたユーザの個人認証情報を、独自の認証情報データベース17に登録されている認証情報に基づいて認証する。

【0035】図4に、仮パスワードデータベース7に登録される仮パスワードのデータ構造の一例を示す。R11の列には、仮パスワードが登録される。R12の列には、仮パスワード有効期限が登録される。R13の列には、この仮パスワードを登録に用いるユーザ情報データ

ベース8の項を示すポインタが登録される。

【0036】このように、仮パスワードデータベース7は、少なくとも仮パスワードと共にその仮パスワードの有効期限が登録され、認証管理装置21で管理される。

【0037】図5に、ユーザ情報データベース8に登録されるユーザ個人の認証情報のデータ構造の一例を示す。R21の列には、ユーザを一義に示すユーザIDが登録される。R22～R24の列には、R21内のユーザIDに対応するユーザの認証手段毎の認証情報の登録状況が登録される。各R22～R24において、r21の列には、登録フラグが登録される。フラグ1は認証パッケージの認証情報が登録待ち状態であることを示し、フラグ0は登録済みであることを示す。r22の列には、認証情報を登録する際に用いる仮パスワードに対応するポインタ、又は認証情報が登録されている認証情報データベース内のポインタが登録される。NULLはユーザが該認証パッケージを使用しないことを示す。

【0038】このように、ユーザ情報データベース8は、少なくともユーザ毎に複数の認証パッケージに対する登録状況が登録され、認証管理装置21で管理される。

【0039】図6に、認証手段データベース9に登録される認証パッケージの情報のデータ構造を示す。R31の列には、認証パッケージ11～13を一義に示す識別子である認証手段IDが登録される。R32の列には、認証手段IDの示す認証パッケージ11～13の認証処理部16と対応するポインタが登録される。R33の列には、認証手段IDの示す認証パッケージ11～13の登録処理部14と対応するポインタが登録される。R34の列には、認証手段IDの示す認証パッケージ11～13の変更処理部15と対応するポインタが登録される。

【0040】R35の列には、一般の認証（通常の認証）を行うときに、認証処理部16に渡されるしきい値が登録される。なお、NULLはしきい値がない場合を示す。R36の列には、認証情報変更時の認証を行うときに、認証処理部16に渡されるしきい値が登録される。なお、NULLはしきい値がない場合を示す。R37の列には、R35及びR36以外で認証処理部16に渡されるパラメタ値が登録される。なお、NULLはパラメタ値がない場合を示す。

【0041】このように、認証手段データベース9は、少なくとも認証手段毎の一般認証時のしきい値と認証情報変更時のしきい値とを区別して登録され、認証管理装置21で管理される。

【0042】図7に、端末情報データベース10に登録される認証条件のデータ構造を示す。R41の列には、端末を一義に示す識別子である端末IDが登録される。R42の列には、端末毎に通常の認証に用いるの認証条件を示す一般認証式が登録される。R43～R44の列

には、それぞれ特定のサービスやアプリケーション専用の認証条件を示す特定認証式が登録される。

【0043】このように、端末情報データベース10は、少なくとも端末毎に通常の認証で用いる認証条件と特定のサービスやアプリケーションで用いる認証条件とを区別して登録され、認証管理装置21で管理される。

【0044】次に、動作について説明する。まず、新たな認証パッケージを認証管理装置21に登録する際の動作について説明する。図8は、認証パッケージを登録する際の処理の流れを示すフローチャートである。

【0045】管理者がデータベース管理部1に認証パッケージの追加を指示すると、処理がスタートする。まず、STEP1で、データベース管理部1は、認証手段データベース9に新たな行を追加する。例えば、図6におけるG33を追加し、G33-R31に登録する認証パッケージに対応する認証手段IDを登録する。この例では“声紋”を登録する。

【0046】STEP2で、データベース管理部1は、続いてG33-R32、G33-R33、G33-R34のそれぞれに、認証パッケージ11の認証処理部16、登録処理部14、変更処理部15のポイントを登録する。

【0047】STEP3で、データベース管理部1は、さらにG33-R35に一般認証しきい値を登録する。例えば、しきい値は管理者によって指定された値を登録する。バイOMETRICSによる個人認証の場合、認証情報と登録されている情報がしきい値以上一致した場合、認証OKとされる。そのため、しきい値が高いほど他人によるなりぞましは難しくなるが、本人が拒否される確率も高くなる。

【0048】STEP4で、データベース管理部1は、さらにG33-R36に変更時認証しきい値を登録する。この値についても、例えば、管理者によって指定された値を登録する。このとき、一般認証しきい値と区別して、より高い値を登録することにより、通常の認証時のセキュリティ強度と認証情報変更時の認証時のセキュリティ強度とを区別することができる。

【0049】STEP5で、データベース管理部1は、さらにG33-R37にその他のパラメータを登録し、処理を終了する。なお、このパラメータ値は、認証実施時に、認証処理振り分け部13が認証パッケージ11の認証処理部16にそのまま渡す値である。

【0050】このように、管理者がデータベース管理部1に認証パッケージの追加を指示すると、データベース管理部1によって、登録する認証パッケージに対応する認証手段IDが認証手段データベース9に登録され、認証関数R32の項目、登録関数R33の項目などが登録される。さらに、一般認証しきい値と変更時認証しきい値とを区別して、例えば、管理者によって指定されたしきい値がそれぞれ設定され、認証パッケージを認証管理

装置21に登録できる。

【0051】次に、新たな端末を認証管理装置21に登録する際の動作について説明する。図9は、端末を登録する際の処理の流れを示すフローチャートである。

【0052】管理者がデータベース管理部1に端末の追加を指示すると、処理がスタートする。まず、STEP6で、データベース管理部1は、端末情報データベース10に新たな行を追加する。例えば、図7におけるG45を追加し、G45-R41に登録する端末を一義に示す端末IDを設定する。この端末IDは、必ずしも1端末に1つ設定する必要はない。例えば、図3におけるパソコンI11とI12のように、同様の動作を行う端末については、グループとして1つの端末IDを設定する。この例では“パソコン2”を設定する。

【0053】STEP7で、データベース管理部1は、続いてG45-R42に一般認証式を登録する。例えば、管理者によって指定された一般認証式を登録する。この一般認証式は、この端末において行われる通常の認証に対する認証条件を示す。また、一般認証式は、AND及びORを用いて自由に設定可能としてもよい。例えば、G41-R42は、ユーザIDと指紋による認証か、又はIDカードでの認証を許すものである。

【0054】STEP8で、データベース管理部1は、さらにG45-R43～R44に特定認証式を登録し、処理を終了する。この式についても、例えば、管理者によって指定された特定認証式を登録する。特定認証式は、特定のアプリケーションに対する認証で用いる認証式であり、“アプリケーションID＝認証式”の書式であらわす。アプリケーションIDは、端末内で認証を必要とするアプリケーションを一意に示す識別子である。また、特定認証式は、アプリケーション毎に複数設定可能であり、特定認証式が複数ある場合は左詰で登録し、すべての登録が終了したら、G44-R44のようにNULLを登録する。

【0055】右辺にNULLを登録した場合は、そのアプリケーションIDの認証はすべてNGとなり、その端末でのアプリケーションの使用の禁止を示す。また、特定認証式は一般認証式と同様に、AND及びORを用いて自由に設定可能としてもよい。こうして端末毎に、また、その端末内のアプリケーション毎に認証式を区別して登録する。

【0056】このように、管理者がデータベース管理部1に端末の追加を指示すると、データベース管理部1によって、登録する端末に対応する端末IDが端末情報データベース10に登録される。さらに、例えば、管理者によって指定された認証手段を任意に組み合わせた認証条件である認証式が、端末毎、アプリケーション毎に区別されて、それぞれ一般認証式R42の項目、特定認証式R43の項目などに登録され、端末を認証管理装置21に登録できる。

【0057】次に、新たなユーザを認証管理装置21に登録する際の動作について説明する。図10は、ユーザに登録する際の処理の流れを示すフローチャートである。

【0058】管理者がデータベース管理部1にユーザの追加を指示すると、処理がスタートする。まず、STEP9で、データベース管理部1は、ユーザ情報データベース8に新たな行を追加する。例えば、図5におけるG23を追加し、G23-R21にそのユーザを一義に示すユーザIDに登録する。この例では“User3”に登録する。

【0059】STEP10で、データベース管理部1は、登録フラグを1に設定する。例えば、ユーザが使用する認証手段として指紋と声紋の登録を行う場合、指紋R22の登録フラグG23-r21と、声紋R23の登録フラグG23-r21を1に設定する。登録フラグはその列における認証手段の認証情報の登録状態を示すものであり、1は登録待ち状態を示し、0は登録済み状態を示す。

【0060】STEP11で、データベース管理部1は、仮パスワードデータベース7に新たな行を追加する。例えば、図4におけるG11を追加し、G11-R11にSTEP10で登録フラグに1を設定した認証情報に対する仮パスワードに登録する。

【0061】STEP12で、さらにデータベース管理部1は、その仮パスワードに対応する有効期限をG11-R11に登録し、STEP13で、ユーザ情報データベースのG23-R22のポインタをG11-R13に登録する。

【0062】STEP14で、仮パスワードのポインタをユーザ情報データベース8に登録する。例えば、G11のポインタをG23-r22に登録する。同様のSTEP11からSTEP14の処理を各列について行う。最後に、STEP15で、仮パスワードをユーザに通知し、処理を終了する。

【0063】このように、管理者がデータベース管理部1にユーザの追加を指示すると、データベース管理部1によって、登録するユーザに対応するユーザIDがユーザ情報データベースに登録される。このときユーザIDは、仮パスワード及びその有効期限と関連付けられて登録され、ユーザに仮パスワードを通知すると共に、ユーザを認証管理装置21に登録できる。

【0064】次に、端末からのコマンドに対する認証管理装置21の処理について説明する。端末から送信されるコマンドには、登録コマンド、変更コマンド、認証コマンドがある。図11は、端末からのコマンドを認証管理装置21が受信した際の処理の流れを示すフローチャートである。

【0065】端末から発信されたコマンドは、ネットワーク28を介して、ネットワーク通信部3に到達する。

ネットワーク通信部3がコマンドを受信するとコマンドに対する処理がスタートする。

【0066】STEP16で、ネットワーク通信部3は、受信したコマンドが登録コマンド、変更コマンド又は認証コマンドのどのコマンド種別であるかを判別する。判別結果が登録コマンドである場合は、同時に受信した端末ID、ユーザID、認証手段ID、認証情報、仮パスワードと共に、登録処理を登録処理振り分け部5に依頼し、STEP17に進む。

【0067】判別結果が変更コマンドである場合は、同時に受信した端末ID、ユーザID、変更用の認証手段IDと認証情報、認証用の認証手段IDと認証情報と共に、変更処理を変更処理振り分け部6に依頼し、STEP30に進む。なお、認証用の認証手段IDと認証情報は、端末から1組以上送信されるものとする。

【0068】また、判別結果が認証コマンドである場合は、同時に受信した端末ID、ユーザID、認証手段ID、アプリケーションID、認証情報と共に、認証処理を認証処理振り分け部4に依頼し、STEP40に進む。なお、この時、ユーザIDとアプリケーションIDはなくともよい。また、認証手段IDと認証情報は、1組以上送信されるものとする。

【0069】まず、登録コマンドの場合について説明する。STEP17で、登録処理振り分け部5は、ユーザ情報データベース8を検索して、ユーザIDとマッチする行を探す。例えば、受信したユーザIDがUser3の場合、図5においてG23がマッチする。

【0070】STEP18で、登録処理振り分け部5は、G23-r21の登録フラグが1、かつG23-r22のポインタがNULLでないかを判定する。その結果、登録フラグが1で、ポインタがNULLでない場合、すなわち、認証情報の登録待ち状態であり、かつ仮パスワードのポインタがNULLでない場合は、STEP19に進む。それ以外の場合は、STEP24に進む。

【0071】STEP19で、登録処理振り分け部5が仮パスワード認証処理部2にG23-r22のポインタを渡して仮パスワードの認証を依頼すると、仮パスワード認証部2は、受信した仮パスワードとG11-R11を用いて仮パスワード認証を行い、仮パスワードを判定する。判定結果がOKの場合は、STEP20に進み、NGの場合は、STEP24に進む。

【0072】STEP20で、登録処理振り分け部5が認証手段データベース9から受信した認証手段IDと一致する行の登録関数R33のポインタを検索し、そのポインタ、受信したユーザID及び認証情報を用いて認証パッケージ11の登録処理部14に登録を依頼すると、登録処理部14はその認証情報を認証パッケージ内の認証データベース17に登録する。このとき、登録処理部14は、リターン値として該当情報の認証情報データベ

ース17内のポインタを登録処理振り分け部5に返す。

【0073】STEP21で、登録処理振り分け部5の依頼を受けて仮パスワード認証処理部は、仮パスワードデータベース7の該当する行G11を削除する。これにより、削除された仮パスワードは無効となり、使用不可能となる。

【0074】STEP22で、登録処理振り分け部5は、登録処理部14のリターン値をユーザ情報データベース8のG23-r22に登録し、登録フラグG23-r21を0に設定する。

【0075】STEP23で、登録処理振り分け部5は、正常通知をネットワーク通信部3を介して端末IDに対応する端末に送信し、登録コマンドに対する処理を終了する。

【0076】一方、STEP18でN、又はSTEP19でNGの場合は、STEP24で、登録処理振り分け部5は、エラーログを記録し、異常通知をネットワーク通信部3を介して端末IDに対応する端末に送信し、登録コマンドに対する処理を終了する。

【0077】次に、変更コマンドの場合について説明する。STEP30で、変更処理振り分け部6は、ユーザID、認証用の認証手段IDと認証情報をもって、認証処理振り分け部4に認証依頼をする。

【0078】STEP31で、変更処理振り分け部6は、認証処理振り分け部4による認証結果を確認する。認証結果がOKの場合はSTEP32に進み、認証結果がNGの場合はSTEP36に進む。

【0079】STEP32で、変更処理振り分け部6は、ユーザ情報データベース8を検索して、ユーザIDに該当する認証情報のポインタの行を検索する。さらに、STEP33で、変更処理振り分け部6は、認証手段データベース9を検索して、変更用の認証手段IDに該当する変更関数の行を検索する。

【0080】STEP34で、変更処理振り分け部6は、変更関数ポインタR33、認証情報のポインタr22及び変更用の認証情報をもって変更処理部14に認証情報の変更を依頼する。これを受けて変更処理部14は、認証情報データベース17内のユーザの認証情報を変更用の認証情報に書き換える。

【0081】STEP35で、変更処理振り分け部6は、正常通知をネットワーク通信部3を介して端末IDに対応する端末に送信し、変更コマンドに対する処理を終了する。

【0082】一方、STEP31でNGの場合は、STEP36で、変更処理振り分け部6は、エラーログを記録し、異常通知をネットワーク通信部3を介して端末IDに対応する端末に送信し、変更コマンドに対する処理を終了する。

【0083】次に、認証コマンドの場合について説明する。STEP40で、認証処理振り分け部4は、認証処

理を行う。この詳細は、図12を使って、別途説明する。

【0084】STEP41で、認証結果を確認する。認証結果がOKならSTEP42で、認証処理振り分け部4は、正常通知と共に認証OKをネットワーク通信部3を介して端末IDに対応する端末に送信し、認証コマンドに対する処理を終了する。

【0085】一方、STEP41で認証結果がNGならSTEP43で、認証処理振り分け部4は、エラーログを記録し、異常通知をネットワーク通信部3を介して端末IDに対応する端末に送信し、認証コマンドに対する処理を終了する。

【0086】次に、STEP40の認証処理の詳細を説明する。図12は、認証処理の詳細な処理の流れを示すフローチャートである。まず、STEP50で、認証処理振り分け部4は、端末情報データベース10を検索して受信した端末IDと一致する行を検索する。

【0087】STEP51で、認証処理振り分け部4は、アプリケーションIDから該当する認証式を決定する。アプリケーションIDが指定されない場合は、一般認証式とする。STEP52で、認証式にマッチする認証IDと認証情報を端末から受信しているかどうかをチェックする。OKの場合はSTEP53に進み、NGの場合はSTEP62に進む。

【0088】STEP53で、認証処理振り分け部4は、認証手段データベース9を検索して受信した認証手段IDと一致する行を検索し、STEP54で、コマンド種別を判別する。認証コマンドの場合はSTEP55で、一般認証しきい値を選択し、変更コマンドの場合はSTEP56で、変更時認証しきい値を選択する。

【0089】STEP57で、認証処理振り分け部4は、ユーザ情報データベースをユーザIDと認証手段IDで検索し、該当するポインタr22を検索する。ユーザIDが指定されていない場合は、ポインタ値はNULLとする。

【0090】STEP58で、認証処理振り分け部4は、STEP55～57で検索したしきい値とポインタ値で、認証関数ポインタR32を用いて該当する認証パッケージ11の認証処理部16をコールする（認証処理を依頼する）。これを受けて、認証処理部16は認証を実施し、結果を認証処理振り分け部4に返す。

【0091】STEP59で、認証処理振り分け部4は、認証処理部16の認証結果を確認する。認証結果がOKの場合はSTEP60に進み、認証結果がNGの場合はSTEP62に進む。

【0092】さらに、STEP60で、認証処理振り分け部4は、認証式が成立したか否かを確認する。認証式が成立しない場合は、成立するまでSTEP53から次の認証手段IDと認証情報について認証処理を繰り返す。一方、認証式が成立する場合は、STEP61に進

み、認証OKとして、認証処理を終了する。

【0093】また、STEP52又はSTEP59でNGの場合は、STEP62に進み、認証NGとして、認証処理を終了する。

【0094】このように、ユーザが端末を用いてサービスを受ける場合、ネットワーク通信部3によってコマンドが判別され、そのコマンドに応じて処理がなされる。例えば、ユーザが認証情報を登録する際は、ネットワーク通信部3によって登録コマンドが判別され、登録処理振り分け部5の指示によって、仮パスワードによる認証がなされた後、所定の認証パッケージにユーザの認証情報が登録されて、ユーザの認証情報を登録することができる。また同時に、仮パスワードデータベース7から使用した仮パスワードが削除され、以降その仮パスワードは使用できなくなる。

【0095】また、ユーザが認証情報を変更する際は、ネットワーク通信部3によって変更コマンドが判別され、変更処理振り分け部6の指示によって、所定の認証パッケージの認証情報が変更される。この時、認証手段データベース10に登録されたしきい値に従って、一般の認証より厳しい認証がなされて、ユーザの認証情報を変更することができる。

【0096】また、ユーザが認証を依頼する際は、ネットワーク通信部3によって認証コマンドが判定され、認証処理振り分け部4の指示によって、認証手段データベース10に登録されたしきい値に従って、認証情報変更時の認証より緩い認証がなされて、個人の判別(認証)をすることができる。

【0097】次に、仮パスワード認証処理部2における仮パスワードの有効期限確認の際の処理について説明する。図13は、仮パスワードの有効期限確認の際の仮パスワード認証処理部2の処理の流れを示すフローチャートである。

【0098】一定時間毎に自動的に処理がスタートする。まず、STEP70で、仮パスワード認証処理部2は、仮パスワードのポインタに基づいて仮パスワードデータベース7の有効期限R11を検索し、その有効期限を確認する。その結果、有効期限内であるときは、そのまま処理を終了する。

【0099】一方、有効期限を過ぎている場合は、STEP72に進み、仮パスワード認証処理部2が登録処理振り分け部5に対して仮パスワードの認証NGを通知すると、登録処理振り分け部5は、ユーザ情報データベース8内のユーザ情報データポインタR13が示すポインタ(r22)をNULLに変える。

【0100】また、STEP72で、仮パスワード認証処理部2は、有効期限を過ぎた仮パスワードデータベース7のその行を削除し、処理を終了する。仮パスワード認証処理部2及び登録処理振り分け部は、以上の処理をすべての行について、定期的に行い、確認する。

【0101】このように、認証情報を登録する際に用いる仮パスワードは、仮パスワードデータベース7に登録された有効期限によって管理され、有効期限が切れると自動的に使用できなくなる。

【0102】以上のように、本実施の形態に係る認証管理装置によれば、端末毎に通常の認証で用いる一般用の認証条件と、特定のサービスやアプリケーションで用いる認証条件とを区別して、複数の認証手段を任意に組み合わせた認証条件が登録される端末情報データベースを備えることにより、様々なサービスを提供する複数の端末やアプリケーションによる異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全てのシステムやアプリケーションに対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0103】また、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデータベースから仮パスワードを削除することにより、例えば、ユーザが何らかの理由で長時間認証情報の登録を行わないときに自動的に登録が不可能となり、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0104】また、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理することにより、認証情報変更時の認証を通常の認証より厳しくできる。例えば、よく似た他人によるバイオメトリックスの認証情報の変更を困難にでき、高度なセキュリティを必要とする場合に適用できる。

【0105】また、認証情報のうち少なくとも一つはバイオメトリックスの認証情報を用いることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【0106】さらにまた、本実施の形態に係る認証管理システムによれば、端末毎に通常の認証で用いる一般用の認証条件と、特定のサービスやアプリケーションで用いる認証条件とを区別して、複数の認証手段を任意に組み合わせた認証条件が登録される端末情報データベースを備える認証管理装置を有することにより、様々なサービスを提供する複数の端末やアプリケーションによる異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全てのシステムやアプリケーションに対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0107】また、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデータベースから仮パスワードを削除する認証管理装置を有することにより、例えば、ユーザが何らかの理由で長時間認証情報の登録を行わないときに自動的に登録が不可能となり、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0108】また、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理する認証管理装置を有することにより、認証情報変更時の認証を通常の認証より厳しくできる。例えば、よく似た他人によるバイオメトリクスの認証情報の変更を困難にでき、高度なセキュリティを必要とする場合に適用できる。

【0109】また、認証情報のうち少なくとも一つはバイオメトリクスの認証情報を用いることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【0110】なお、本実施の形態では、仮パスワードは有効期限内は常に有効である場合について説明したが、さらに、有効となる条件として時刻や端末の条件を加えてもよい。これにより、さらにセキュリティを向上できる。例えば、有効条件として、特定時刻の8時から17時と特定端末のドア制御とを追加することにより、認証情報の登録は、管理者が監視できる時刻の8時から17時にドア制御の端末からしか行えなくなる。

【0111】また、本実施の形態では、認証のしきい値のみで認証情報変更時の認証と通常の認証とを区別する場合について説明したが、さらに、認証処理を実施する時刻やコマンドを発行する端末の条件を付けてもよい。これにより、さらにセキュリティを向上できる。例えば、認証情報の変更は、8時から17時までに特定の端末からしか行えないようにすることができる。

【0112】また、本実施の形態では、認証情報の登録には常に仮パスワードを用いる場合について説明したが、既に登録されている別の種類の認証情報がある場合は、認証情報の変更と同じように、その認証情報で変更時認証用しきい値を用いて認証するようにしてもよい。これにより、仮パスワードを使用する機会を減少でき、よりセキュリティを向上できる。また、既に登録されている認証情報を用いて別の認証情報を登録する際の有効期限を設けてもよく、本実施の形態と同様の効果が得られる。例えば、新たに声紋の認証情報を登録する際に、既に登録されている指紋の認証情報を用いて認証して声

紋の認証情報を登録する。また、指紋の認証情報に対して、登録のための認証に用いる場合の有効期限を設ける。

【0113】

【発明の効果】以上のように、本発明の認証管理装置によれば、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースを備えることにより、異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全ての認証方式に対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0114】また、本発明の認証管理装置によれば、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデータベースから仮パスワードを削除することにより、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0115】また、本発明の認証管理装置によれば、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理することにより、例えば、認証情報変更時の認証を通常の認証より厳しくでき、高度なセキュリティを必要とする場合に適用できる。

【0116】また、本発明の認証管理装置によれば、認証情報の少なくとも一つはバイオメトリクスの認証情報であることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【0117】さらにまた、本実施の認証管理システムによれば、認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報データベースを備える認証管理装置を有することにより、異なる認証方式を同一の認証管理装置を使用して一括して設定でき、管理者の作業を容易にできると共に、管理者が全ての認証方式に対して統一したセキュリティ・ポリシーのもとに認証条件を設定し、管理できる。

【0118】また、本発明の認証管理装置システムによれば、ユーザの認証情報を登録する際に参照される仮パスワードとその仮パスワードの有効期限とを関連付けて登録される仮パスワードデータベースを備え、有効期限に応じて又は認証情報の登録に応じて仮パスワードデータベースから仮パスワードを削除する認証管理装置を有することにより、不正な認証情報の登録を回避でき、高度なセキュリティを必要とする場合に適用できる。

【0119】また、本発明の認証管理装置システムによれば、認証手段毎に通常の認証で用いる一般認証時のしきい値と、認証情報を変更する際に用いる認証情報変更時のしきい値とを区別して登録できる認証手段データベースを備え、通常の認証には一般認証時のしきい値を用い、認証情報を変更する際には認証情報変更時のしきい値を用いて認証処理する認証管理装置を有することにより、例えば、認証情報変更時の認証を通常の認証より厳しくでき、高度なセキュリティを必要とする場合に適用できる。

【0120】また、本発明の認証管理装置システムによれば、認証情報の少なくとも一つはバイオメトリクスの認証情報であることにより、より厳密に個人認証することができ、高度なセキュリティを必要とする場合に適用できる。

【図面の簡単な説明】

【図1】 この発明の実施の形態1における認証管理装置の構成を示すブロック図。

【図2】 この発明の実施の形態1における認証管理システムのシステム構成を示すブロック図。

【図3】 この発明の実施の形態1における認証管理システムの具体的なシステム構成を示すブロック図。

【図4】 この発明における仮パスワードデータベースのデータ構成を示す図表。

【図5】 この発明のユーザ情報データベースのデータ構成を示す図表。

【図6】 この発明の認証手段データベースのデータ構成を示す図表。

【図7】 この発明の端末情報データベースのデータ構成を示す図表。

【図8】 この発明の認証パッケージの登録手順を示すフローチャート。

【図9】 この発明の端末の登録手順を示すフローチャート。

【図10】 この発明のユーザの登録手順を示すフローチャート。

【図11】 この発明の端末からのコマンドに対する処理手順を示すフローチャート。

【図12】 この発明の認証処理の処理手順を示すフローチャート。

ーチャート。

【図13】 この発明の仮パスワードの有効期限の確認処理の処理手順を示すフローチャート。

【図14】 従来の認証機能を備えたサービス・サーバのシステム構成を示すブロック図。

【符号の説明】

1 データベース管理部	2 仮パスワード認証処理部
3 ネットワーク通信部	4 認証処理振り分け部
5 登録処理振り分け部	6 変更処理振り分け部
7 仮パスワードデータベース情報データベース	8 ユーザ情報データベース
9 認証手段データベース情報データベース	10 端末
11～13 認証パッケージ処理部	14 登録処理部
15 変更処理部	16 認証処理部
17 認証情報データベース管理装置	21 認証管理装置
22～24 端末	25～27 インタフェース装置
28 ネットワーク管理装置	A1 認証管理装置
C1 出退勤管理装置	C2、C3 ドア制御装置
C4 勤怠管理装置	C5 メールサーバ
I1 テンキーパット	I2～I6 指紋取得装置
I7～I9 ICカードリーダ	I10 声紋取得装置
I11～I15 パソコン	31 サービス処理部
32 認証処理部	33 認証情報データベース
34 登録サービス処理部	

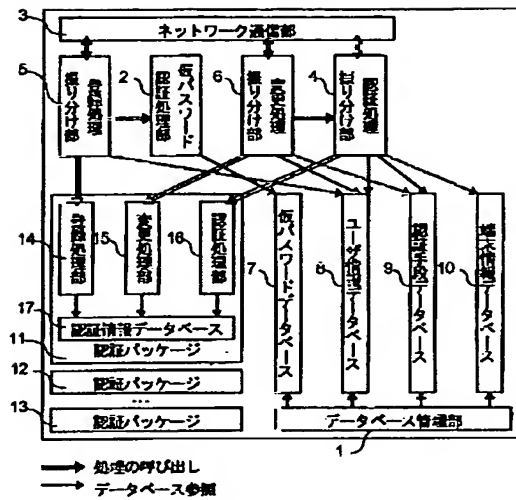
【図4】

	R11	R12	R13
G11	仮パスワード	有効期限	ユーザ情報データポイント
G12			ポイント
			ポイント

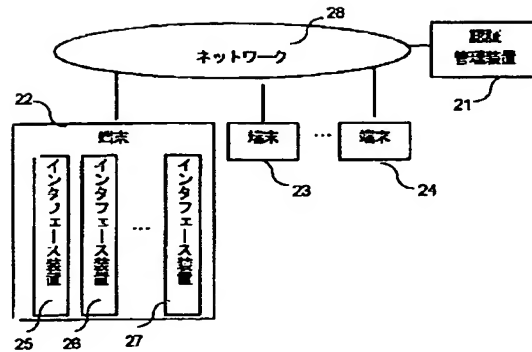
【図5】

	R21	R22	R23	R24
G21	ユーザID	指紋	声紋	パスワード
G22	User1	0 ポイント	0 ポイント	0 NULL
G23	User2	0 ポイント	0 ポイント	0 ポイント
	User3	1 ポイント	1 ポイント	0 NULL
	...			

【図1】



【図2】



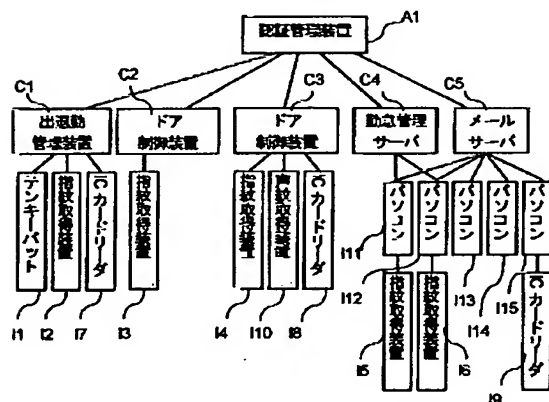
【図6】

	R31	R32	R33	R34	R35	R36	R37
	認証 手段 ID	認証 関数	登録 関数	変更 関数	一般 認証 しきい 値	変更時 認証 しきい 値	その他 パラ メタ
G31	パス ワード	ポイン タ	ポイン タ	ポイン タ	NULL	NULL	NULL
G32	指紋	ポイン タ	ポイン タ	ポイン タ	値	値	値
G33	声紋	ポイン タ	ポイン タ	ポイン タ	値	値	NULL
...							

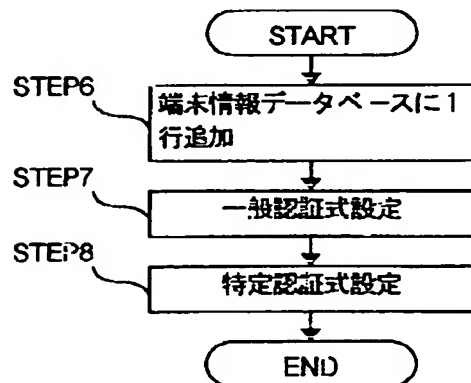
【図7】

	R41	R42	R43	R44
	端末 ID	一般認証式	特定 認証式 1	特定 認証式 2
G41	出退勤 管理装置	(ユーザ ID * 指紋) + IC カード	NULL	
G42	ドア制御 装置 1	指紋	NULL	
G43	ドア制御 装置 2	(指紋 * IC カード) + (声紋 * IC カード)	NULL	
G44	パソコン 1	ユーザ ID *	勤怠管理 = ユーザ ID *	NULL
G45	パソコン 2	パスワード IC カード *	勤怠管理 = NULL	NULL
...				

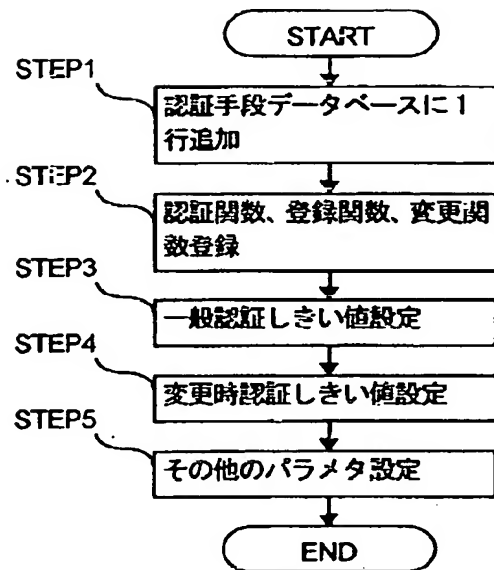
【図3】



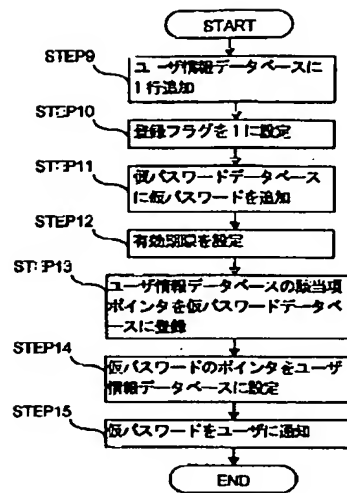
【図9】



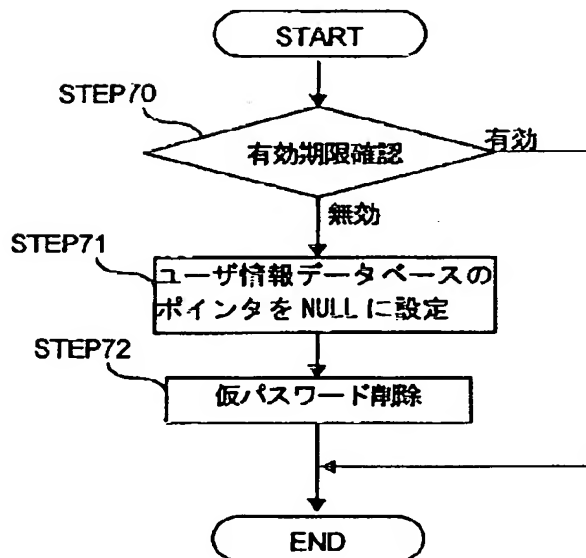
【図8】



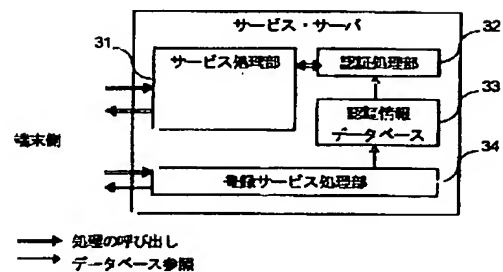
【図10】



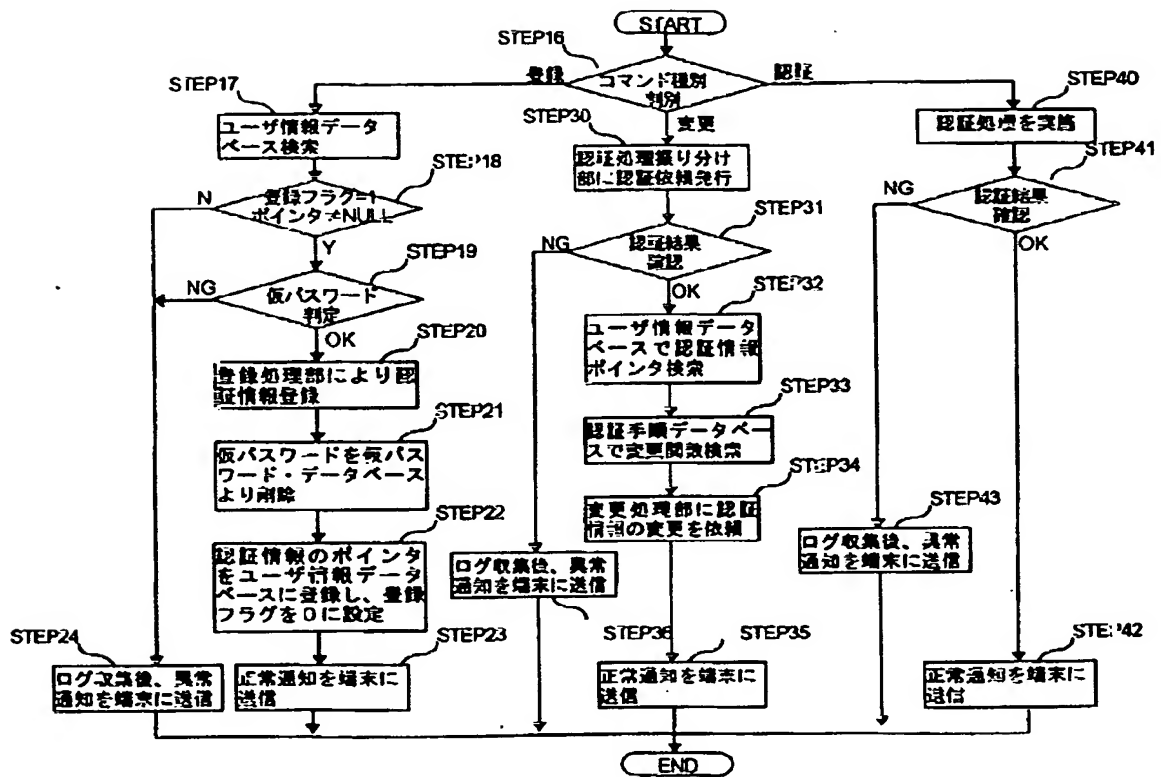
【図13】



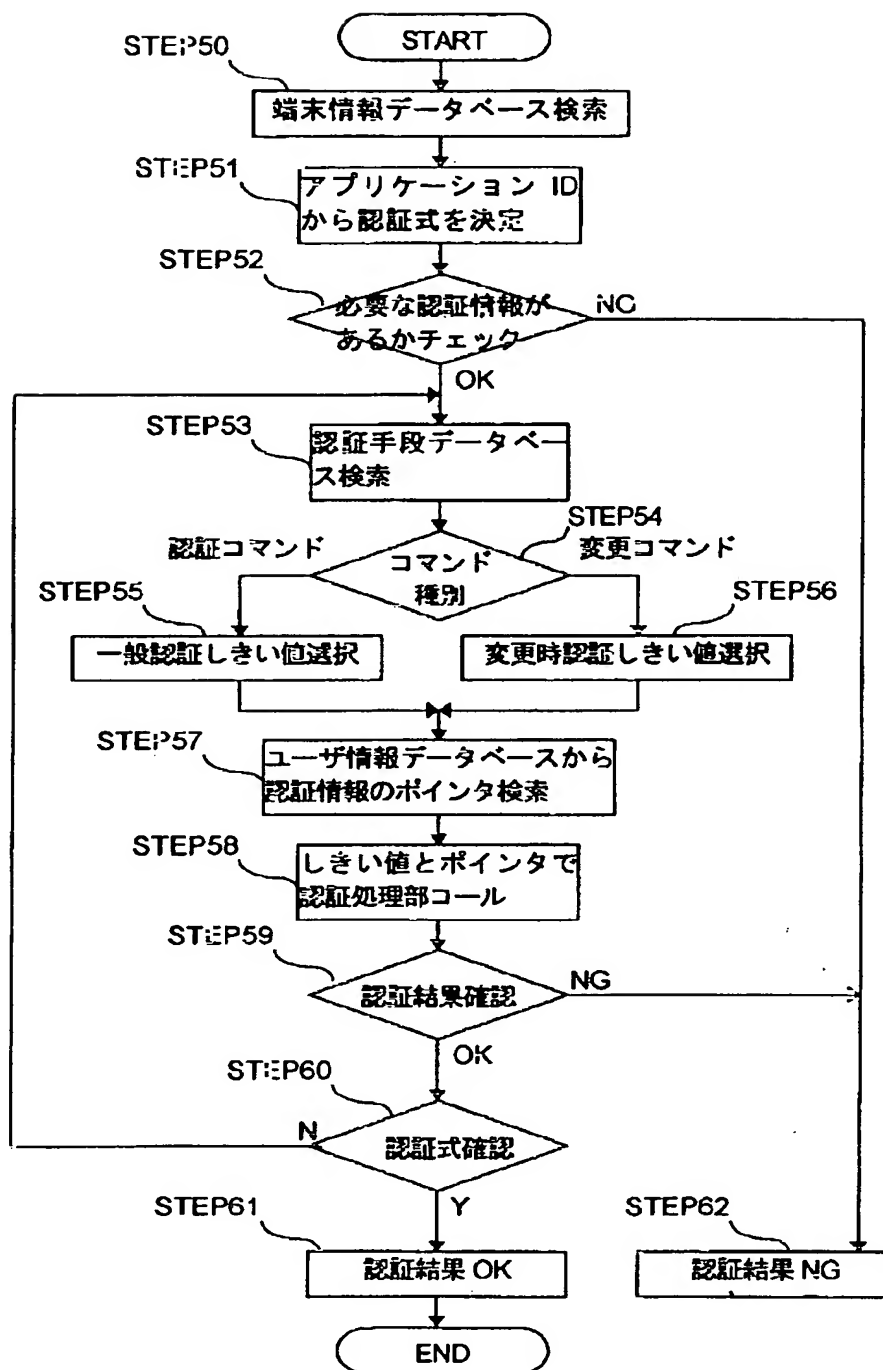
【図14】



【図11】



【図12】



フロントページの続き

(72) 発明者 馬場 義昌
東京都千代田区丸の内二丁目 2 番 3 号 三
菱電機株式会社内